



# FortiSwitch Release Notes

Version 6.0.4

## **FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

## **FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

## **FORTIGUARD CENTER**

<http://www.fortiguard.com>

## **FORTICAST**

<http://forticast.fortinet.com>

## **END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

## **FORTINET PRIVACY POLICY**

<https://www.fortinet.com/corporate/about-us/privacy.html>

## **FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



FortiSwitch Release Notes

September 22, 2019

11-604-536628-20190922

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Supported models	5
What's new in FortiSwitchOS 6.0.4	5
<b>Special notices</b>	<b>7</b>
Supported features for FortiSwitchOS 6.0	7
Connecting multiple FSW-R-112D-POE switches	13
<b>Upgrade information</b>	<b>14</b>
Cooperative Security Fabric upgrade	14
<b>Product integration and support</b>	<b>15</b>
FortiSwitch 6.0.4 support	15
<b>Resolved issues</b>	<b>16</b>
<b>Known issues</b>	<b>17</b>

## Change log

Date	Change Description
May 16, 2019	Initial release for FortiSwitchOS 6.0.4
June 11, 2019	Added bug 528983 to the “Known issues” section.
July 22, 2019	Added bug 572052 to the “Known issues” section.
September 22, 2019	Updated the feature matrix (TDR and split port rows).

# Introduction

This document provides the following information for FortiSwitch 6.0.4 build: 0064.

- [Supported models on page 5](#)
- [Special notices on page 7](#)
- [Upgrade information on page 14](#)
- [Product integration and support on page 15](#)
- [Resolved issues on page 16](#)
- [Known issues on page 17](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

## Supported models

FortiSwitch 6.0.4 supports the following models:

<b>FortiSwitch 1xx</b>	FSW-108E, FSW-108E-POE, FSW-108E-FPOE, FSW-124E, FSW-124E-POE, FSW-124E-FPOE, FSW-148E, FSW-148E-POE
<b>FortiSwitch 2xx</b>	FSW-224D-FPOE, FSW-224E, FSW-224E-POE, FSW-248D, FSW-248E-POE, FSW-248E-FPOE
<b>FortiSwitch 4xx</b>	FSW-424D, FSW-424D-FPOE, FSW-424D-POE, FSW-448D, FSW-448D-FPOE, FSW-448D-POE
<b>FortiSwitch 5xx</b>	FSW-524D-FPOE, FSW-524D, FSW-548D, FSW-548D-FPOE
<b>FortiSwitch 1xxx</b>	FSW-1024D, FSW-1048D, FSW-1048E
<b>FortiSwitch 3xxx</b>	FSW-3032D, FSW-3032E
<b>FortiSwitch Rugged</b>	FSR-112D-POE, FSR-124D

## What's new in FortiSwitchOS 6.0.4

Release 6.0.4 provides the following new features and changes:

- When loop guard is triggered, "Triggered" is displayed in the Status column on the *Switch > Monitor > Loop Guard* page.
- The dashboard displays when the FortiSwitch unit is managed by FortiSwitch Cloud.
- A new column on the *System > Network > Interface > VLAN* page shows the VLAN IDs.
- A new column on the *Switch > Interface > Trunk* page shows the traffic over the last day.

- FortSwitch 6.0.4 GA will support the following:
  - `acct-fast-framedip-detect` timer setting
  - `framed-mtu-size` RADIUS attribute
  - `service-type` RADIUS attribute
- You can configure the Framed-IP-Address detection timer to control how quickly IP addresses are discovered and reported.
- The `set source-ip` command under `config acct-server` has been removed. The source IP address configured under the `config user radius` command will be used for the accounting server.
- The `set eap-passthru` command is now enabled by default.
- The `set security-mode` command has been removed from under the `config switch interface` command.

# Special notices

## Supported features for FortiSwitchOS 6.0

The following table lists the FortiSwitch features in Release 6.0 that are supported on each series of FortiSwitch models. All features are available in Release 6.0.0, unless otherwise stated.

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
<b>Management and Configuration</b>							
CPLD software upgrade support for OS	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support) (release 3.6.0)	—	✓	148E 148E-POE	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓
Support for switch SNMP OID	✓	✓	✓	✓	✓	✓	✓
IP conflict detection and notification	✓	✓	✓	✓	✓	✓	✓
<b>Security and Visibility</b>							
802.1x port mode	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
802.1x enhancements, including MAB (release 3.5.1)	✓	✓	✓	✓	✓	✓	✓
MAB reauthentication disabled (release 3.6.4)	—	✓	—	✓	✓	✓	✓
open-auth mode (release 6.0.0)	✓	✓	✓	✓	✓	✓	✓
Support of the RADIUS accounting server (release 3.6.3)	Partial	✓	—	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages (release 3.6.3)	—	✓	—	✓	✓	✓	✓
EAP Pass-Through (release 3.6.3)	✓	✓	—	✓	✓	✓	✓
Network device detection (release 3.6.2)	—	—	—	✓	✓	✓	✓
IP-MAC-Binding	✓	—	—	—	✓	✓	✓
sFlow	✓	✓	—	✓	✓	✓	✓
ACL	—	—	—	✓	✓	✓	✓
Multistage ACL (release 6.0.0)	—	—	—	—	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓
DHCP blocking (release 6.0.0)	—	—	—	✓	—	—	—
Dynamic ARP inspection (release 3.6.0)	✓	—	—	✓	✓	✓	✓



Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
ARP timeout value (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
Access VLANs (See Note 5.)	—	—	—	✓	✓	✓	✓
VLAN tag by ACL	—	—	—	✓	✓	✓	✓
<b>Layer 2</b>							
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	24/48	24/48	24 (3.5.0) 64 (3.5.1)
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓
IGMP snooping	✓	—	—	✓	✓	✓	✓
IGMP querier (release 3.6.4)	—	—	—	✓	✓	✓	✓
LLDP transmit	—	✓	—	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓
Per-port max for learned MACs	—	—	✓	✓	✓	—	—
MAC learning limit (release 3.6.0) (See Note 4.)	—	—	✓	✓	✓	—	—
Learning limit violation log (release 3.6.4) (See Note 4.)	—	—	—	✓	✓	—	—
set mac-violation-timer (release 6.0.0)	—	✓	—	✓	✓	✓	✓
Sticky MAC (releases 3.6.0 and 6.0.0)	✓	✓	✓	✓	✓	✓	✓
Total MAC entries (release 6.0.0)	—	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MSTP	—	✓	✓	✓	✓	✓	✓
STP root guard (release 3.6.2)	—	✓	✓	✓	✓	✓	✓
STP BPDU guard (release 3.6.2)	—	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)	—	✓	—	✓	✓	✓	✓
Private VLANs	✓	—	—	✓	✓	✓	✓
Multi-stage load balancing (release 3.5.1)	—	—	—	—	—	✓	✓
Priority-based flow control (release 6.0.0)	—	—	—	—	—	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓
MAC/IP/protocol- based VLAN assignment	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	—	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓
Percentage rate control (release 6.0.0)	✓	—	—	✓	✓	✓	✓
<b>Layer 3</b>							
Static L3/hardware- based routing	✓	—	—	✓	✓	✓	✓
Software routing only	✓	✓	✓	—	—	—	—
OSPF (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
RIP (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓
VRRP (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓
BGP (release 6.0.0)	—	—	—	—	✓	✓	✓
IS-IS (release 6.0.0)	—	—	—	—	✓	✓	✓
PIM (release 6.0.0)	—	—	—	—	✓	✓	✓
Hardware-based ECMP	—	—	—	—	✓	✓	✓
Static BFD	—	—	—	—	—	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓
<b>High Availability</b>							
MCLAG (multichassis link aggregation) (release 3.6.0)	Partial	—	—	✓	✓	✓	✓
STP supported in MCLAGs (release 3.6.4)	—	—	—	✓	✓	✓	✓
<b>Quality of Service</b>							
802.1p support, including priority queuing trunk and WRED (release 3.5.1)	✓	—	—	✓	✓	✓	✓
QoS queue counters (releases 3.6.2 and 3.6.3)	—	—	—	✓	✓	✓	✓
QoS marking (release 3.6.4)	—	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Summary of configured queue mappings (release 6.0.1)	✓	—	✓	✓	✓	✓	✓
<b>Miscellaneous</b>							
PoE-pre-standard detection (See Note 1.)	—	✓	FS-1xxE POE	✓	✓	—	—
PoE modes support: first come, first served or priority based (PoE models) (release 3.6.0)	—	✓	FS-1xxE POE	✓	✓	—	—
Control of temperature alerts (release 3.6.4)	—	✓	—	✓	✓	✓	✓
Split port	Partial	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support (release 3.6.0)	✓	—	—	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support) (release 3.6.0)	—	✓	—	✓	✓	✓	✓
Cut-through switching (release 3.6.4)	—	—	—	—	—	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Add CLI to show the details of port statistics (release 3.6.0)	—	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode (release 3.6.4)	—	—	—	—	✓	1048D	✓
Energy-efficient Ethernet (release 6.0.1)	—	✓	✓	✓	✓	—	—

### Notes

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524-FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
3. To use the dynamic layer-3 protocols, you must have an advanced features license.
4. The per-VLAN learning limit and per-trunk learning limit are not supported on dual-chip platforms (448 series).
5. Access VLANs are not supported on 108D-POE, 224D-POE, or 112D-POE.

## Connecting multiple FSW-R-112D-POE switches

The FSW-R-112D-POE switch does not support interconnectivity to other FSW-R-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

# Upgrade information

FortiSwitch 6.0.4 supports upgrading from FortiSwitch 3.5.0 and later.

## Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

# Product integration and support

## FortiSwitch 6.0.4 support

The following table lists 6.0.4 product integration and support information.

<b>Web browser</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11</li><li>• Mozilla Firefox version 52</li><li>• Google Chrome version 56</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS (FortiLink Support)</b>	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

## Resolved issues

The following issues have been fixed in 6.0.4. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
506762	It is difficult to access the switch when an IP camera is connected to port 21.
515211, 534922	Upgrading from FortiSwitchOS 6.0.3 can cause the switch to stop responding.
527565	When MAB is enabled on a FortiSwitch port, you cannot quarantine a host.
529688	After a FortiSwitch unit in FortiLink mode is restarted, the FortiGate unit sends traffic from the LAG port that is down.
530517	There is random ping loss when dynamic ARP inspection (DAI) is enabled on a VLAN.
539957	When MAC authentication bypass (MAG) is enabled on a managed switch's port, clients being authenticated by MAB are moved to unknown VLANs after re-authentication.
541865	The <i>Log &gt; Event Log &gt; System</i> page does not display detailed logs when there are changes made in an admin session.
541871	A managed FortiSwitch unit cannot be reached by SSH when using a public key.
543765	Selecting <i>Revert</i> in the <i>System &gt; Config &gt; Revisions</i> page fails for FS-1xx Series switches running FortiSwitchOS 6.0 or later.
543789	The LLDP MED service has a high memory usage in a core switch in FortiLink mode.
547351	After upgrading from FortiSwitchOS 3.6.9 to 6.0.3, the trunk interface configuration is lost.



# Known issues

The following known issues have been identified with 6.0.4. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
380239	<p>IGMP-snooped multicast groups are not immediately flushed out of the snooping table when the querier port is shut down.</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
382518, 417024, 417073, 417099, 438441	<p>DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).</p>
391607	<p>Switch does not send gratuitous ARP for IP conflict when the system boots up and adds a new switch virtual interface (SVI).</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
414972	<p>IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.</p>
416655	<p>When using DHCP, the IPv6 address cannot be configured. Also, the automatic configuration of the global address does not work.</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>
480605	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"><li>—Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN.</li><li>—Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew &lt;interface&gt;</code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.</li></ul>
488044	<p>On a Protocol Independent Multicast (PIM) topology using the assert mechanism, when the assert winner lost the route to the source, no multicast route was created, and the multicast traffic stopped.</p> <p><b>Workaround:</b> Upgrade to FortiSwitchOS 6.2.0.</p>

Bug ID	Description
510943	<p>When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag &lt;physical port name&gt;</code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p> <p><b>Workaround:</b> When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag &lt;physical port name&gt;</code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
520954	<p>When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.</p>
528983	<p>When IGMP snooping is enabled on a VLAN, reserved multicast packets are forwarded twice on the 124D, 224D-FPOE, 248D, 424D, 424D-POE, 424D-FPOE, 448D, 448D-POE, 448D-FPOE, 224E, 224E-POE, 248E-POE, 248E-FPOE models.</p>
535736	<p>If a FortiSwitch firmware image is an even multiple of 1024 bytes, it will not upgrade properly using the default FortiLink upgrade mechanism. The following builds are known to be affected:</p> <p><b>version 3.x</b> build 0415/FSW_124D_POE</p> <p><b>version 6.x</b> build 0039/FSW_1048E build 0043/FSW_124E build 0141/FSW_224D_FPOE build 0052/FSW_548D_FPOE</p> <p><b>Workarounds:</b></p> <p>—Change to HTTPS mode using the following commands:</p> <pre>config switch-controller global     set https-image-push enable end</pre> <p>—Upgrade to FortiOS 6.0.5 (build 0243 or later) or FortiOS 6.2.0 (build 0794 or later).</p>
572052	<p>Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.</p> <p><b>Workaround:</b> Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>



**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.